Andrew Rutherford

CSCI 4113

Lab 8

All Machines:

1. **ACCEPT** all **ESTABLISHED** or **RELATED** **INPUT** traffic, and traffic from the local loopback adapter **lo**.  (This allows the stateful features of **iptables** to increase both performance and security.  It also allows local traffic in each machine to flow freely.)
   1. Iptables –A INPUT –m conntrack –ctstate ESTABLISHED,RELATED –j ACCEPT
   2. Iptables –I INPUT 1 –i lo –j ACCEPT
   3. Iptables –A OUTPUT –o lo –j ACCEPT
2. **ACCEPT** **INPUT icmp** traffic only of **icmp-type** **echo-request**, **echo-reply** (ping), **time-exceeded** (traceroute), or **destination-unreachable**.  (This lets **ping** and **traceroute** work but drops other commonly abused **icmp** packets.)
   1. iptables –A INPUT –p icmp –icmp-type echo-request –j ACCEPT
   2. iptables –A INPUT –p icmp –icmp-type echo-reply –j ACCEPT
   3. iptables –A INPUT –p icmp –icmp-type time-exceeded –j ACCEPT
   4. iptables –A INPUT –p icmp –icmp-type destination-unreachable –j ACCEPT
3. On all machines, allow **NEW** **inbound ssh**connections **only**from 100.64.0.0/16, 100.64.N.0/24, 100.64.254.0/24, 10.21.32.0/24, and 198.18.0.0/16.  (This limits the subnets from which ssh can be run.)
   1. Iptables –A INPUT –p tcp –s 100.64.0.0/16 –dport 22 –j ACCEPT
   2. Iptables –A INPUT –p tcp –s 100.64.36.0/24 –dport 22 –j ACCEPT
   3. Iptables –A INPUT –p tcp –s 100.64.254.0/24 –dport 22 –j ACCEPT
   4. Iptables –A INPUT –p tcp –s 10.21.32.0/24 –dport 22 –j ACCEPT
   5. Iptables –A INPUT –p tcp –s 198.18.0.0/16 –dport 22 –j ACCEPT
4. On all machines except MachineA/router and MachineC/platen, the *default policy* should be to **DROP** **INPUT** and **FORWARDed** traffic, and **ACCEPT** **OUTPUT** traffic.
   1. Iptables –P INPUT DROP
   2. Iptables –P FORWARD DROP
   3. Iptables –P OUTPUT ACCEPT

Machine A:

1. **DROP FORWARDed** traffic in either direction from Facebook.  You need not block all Facebook IP addresses, just the one you receive from a one-time resolve of facebook.com.    
   To go above and beyond the requirements by blocking all Facebook IP addresses, get a list as follows:   
           root@machineA# **yum install jwhois**  
           root@machineA# **whois -h whois.radb.net '!gAS32934'**
   1. Iptables –A FORWARD –s 157.240.2.35 –j DROP
   2. Iptables –A FORWARD –d 157.240.2.35 –j DROP
2. **DROP** all**FORWARDed** traffic in either direction from icanhas.cheezburger.com and cheezburger.com.  Again, you need not block all such IP addresses, just the ones you receive from a one-time resolve.
   1. Iptables –A FORWARD –s 216.176.177.72 –j DROP
   2. Iptables –A FORWARD –d 216.176.177.72 –j DROP
3. **ACCEPT** **NEW** connections to the given machines based on the rules for each specific machine.  **DROP** all other inbound (e.g. if the input interface is **eth0**) **FORWARDed** traffic .  This is an added layer of security in case the firewall on one of the other machines is inadvertently dropped.
   1. Iptables FORWARD rules added for all rules applied to all machines.
4. MachineA’s *default policies* should be to **DROP** **INPUT** traffic, and **ACCEPT** both **OUTPUT** and **FORWARDed** traffic.
   1. Iptables –P INPUT DROP
   2. Iptables –P OUTPUT ACCEPT
   3. Iptables –P FORWARD ACCEPT

Machines B and F:

1. **ACCEPT** **NEW** **http** and **https** traffic from any source IP.
   1. Iptables –A INPUT –p tcp –dport 80 –m conntrack –ctstate NEW,ESTABLISHED –j ACCEPT
   2. Iptables –A INPUT –p tcp –dport 443 –m conntrack –ctstate NEW,ESTABLISHED –j ACCEPT

Machine C:

1. **ACCEPT** all **INPUT** traffic from 100.64.0.0/16.
   1. Iptables –A INPUT –p tcp –s 100.64.0.0/16 –j ACCEPT
2. Allow **NEW** inbound **ftp**traffic only from 100.64.0.0/16, 100.64.0.27 and 172.20.74.4.
   1. Iptables –A INPUT –p tcp –dport 21 –s 100.64.0.0/16 –j ACCEPT
   2. Iptables –A INPUT –p tcp –dport 21 –s 100.64.0.27 –j ACCEPT
   3. Iptables –A INPUT –p tcp –dport 21 –s 172.20.74.4 –j ACCEPT
3. **ACCEPT** **OUTPUT** **dns**requests to 100.64.N.4 (chase).
   1. Iptables –A OUTPUT –p udp –d 100.64.36.4 –dport 53 –j ACCEPT
4. **ACCEPT** **OUTPUT** **ftp**, **http**, **https,**and **ssh** connections to any host.
   1. Iptables –A OUTPUT –p tcp –sport 21 –j ACCEPT
   2. Iptables –A OUTPUT –p tcp –sport 80 –j ACCEPT
   3. Iptables –A OUTPUT –p tcp –sport 443 –j ACCEPT
   4. Iptables –A OUTPUT –p tcp –sport 22 –j ACCEPT
5. **ACCEPT OUTPUT** **icmp** traffic only for **icmp-type**s **echo-request**, **echo-reply** (ping), **time-exceeded** (**traceroute**), or **destination-unreachable**.
   1. Iptables –A OUTPUT –p icmp –icmp-type 8 –j ACCEPT
   2. Iptables –A OUTPUT –p icmp –icmp-type 0 –j ACCEPT
   3. Iptables –A OUTPUT –p icmp –icmp-type 11 –j ACCEPT
   4. Iptables –A OUTPUT –p icmp –icmp-type 3 –j ACCEPT
6. The *default policy* for **OUTPUT** and **INPUT** should be **DROP**.
   1. Iptables –P INPUT DROP
   2. Iptables –P OUTPUT DROP

Machine D:

1. **ACCEPT NEW dns** queries from any source.
   1. Iptables –A INPUT –p udp –sport 53 –j ACCEPT
   2. Iptables –A INPUT –p udp –dport 53 –j ACCEPT

Machine E:

1. Restrict**NEW** connections to the file sharing services (CIFS and SMB) from the 10.21.32.0/24 network only.  CIFS and SMB use port numbers: 135/tcp, 137-139/udp, and 445/tcp.
   1. Iptables –A INPUT –p tcp –s 10.21.32.0/24 –dport 445 –j ACCEPT
   2. Iptables –A INPUT –p udp –s 10.21.32.0/24 –dport 137 –j ACCEPT
   3. Iptables –A INPUT –p udp –s 10.21.32.0/24 –dport 138 –j ACCEPT
   4. Iptables –A INPUT –p udp –s 10.21.32.0/24 –dport 139 –j ACCEPT
   5. Iptables –A INPUT –p tcp –s 10.21.32.0/24 –dport 135 –j ACCEPT
2. **ACCEPT** **NEW** **ssh** connections only from hosts in the 10.21.32.0/24 subnet and from Machine A.
   1. Iptables –A INPUT –p tcp –s 10.21.32.0/24 –dport 22 –j ACCEPT
   2. Iptables –A INPUT –p tcp –s 100.64.36.1 –dport 22 –j ACCEPT